IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	)	
	)	Examiner: Davis, Zachary A.
Brian J. Matt	)	
	)	Art Unit: 2137
Application No. 09/921,231	)	
	)	
Filed: July 31, 2001	)	
	)	Date: January 10, 2007
For: METHOD AND APPARATUS FOR CRYPTOGRAPHIC KEY ESTABLISHMENT USING AN IDENTITY BASED SYMMETRIC KEYING TECHNIQUE	)	

Issue Fee Payment Transmittal

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith are the following items:

1) Comments on Statement of Reason for Allowance
2) Part B- Issue Fee Transmittal

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Reg. No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
(408) 971-2573

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	
Brian J. Matt	Examiner: Davis, Zachary A.
Application No. 09/921,231	Art Unit: 2137
Filed: July 31, 2001	
For: METHOD AND APPARATUS FOR CRYPTOGRAPHIC KEY ESTABLISHMENT USING AN IDENTITY BASED SYMMETRIC KEYING TECHNIQUE	Date: January 10, 2007

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice of Allowance mailed November 28, 2006, please enter the following:

REMARKS

The Examiner has stated in the Examiner's Statement of Reasons for Allowance that the reasons for allowance were set forth in the Office Action mailed 6/6/06. Applicant notes that in such Office Action, the Examiner stated the following as the reasons for allowance: "Claims 1, 18 and 20 are directed to a method, apparatus, and software implementation of a method performing a cryptographic key establishment protocol," "[t]he protocol includes several messages sent between first and second nodes and a key distribution center," "[t]he protocol further includes node keys created based on node identifiers and secret knowledge, verification of message authentication codes based on the node keys, and verification of hash values of the identifiers combined with nonces," that the "protocol at its most basic level includes the first node requesting from the second node the establishment of a key, the second node requesting a key from the key distribution center (KDC), the KDC generating a shared key and sending the shared key to each node encrypted under the respective node keys, and the nodes establishing with each other that each node has the shared key by exchanging predetermined messages comprising hash values encrypted under the shared key" (emphasis added).

The Examiner has also stated the following: "[the prior art] does not explicitly disclose or implicitly suggest exactly the steps of the protocol of the content of the messages as claimed..."

In response, applicant points out that at least some of the independent claims (e.g. Claims 1, 18 and 20) are not limited to at least the emphasized features that the Examiner has highlighted above.

Just by way of example, at least some of applicant's independent claims are not limited to "node keys created based on node identifiers and secret knowledge" as the Examiner specifically notes (emphasis added). In addition, at least some of applicant's independent claims do not specifically claim "verification of hash values of the identifiers

combined with nonces," as the Examiner further notes (emphasis added). Still yet, at least some of applicant's independent claims are not limited to "nodes establishing with each other that each node has the shared key by exchanging predetermined messages comprising hash values encrypted under the shared key," as the Examiner also notes (emphasis added).

Clearly, at least some of the independent claims are not limited to the features that the Examiner has noted above in the Examiner's Statement of Reasons for Allowance, as emphasized above (by way of example). Instead, each of the claims should only be limited by the language existing therein.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. For payment of the fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAIIP254/01.001.01).

Respectfully submitted,
Zilka-Kotab, P.C.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 505-5100